

Cyber Intrusion Compromise of OPM Personnel Records

June 30, 2015

In June 2015, the Office of Personnel Management (OPM) announced that cyber intrusions had compromised the personnel records of some current and former Federal employees.

OPM has posted detailed information and guidance on its website www.opm.gov (check the “What’s New” section or type “cybersecurity incidents” in the search box). OPM is updating that guidance as new facts are verified.

Below is additional guidance (directed primarily at current employees) that was distributed by the Under Secretary of State for Management on June 29, 2015:

Dear Colleagues,

I am writing to provide a further update on the recent cyber incidents at the U.S. Office of Personnel Management (OPM). OPM is working hard to improve customer service, complete the interagency forensics effort, and conduct a comprehensive IT systems review. We have heard many of your questions and concerns about these incidents which we will address here.

Personnel Records Incident

First, OPM is working to complete the process of notifying individuals whose personally identifiable information (PII) may have been compromised by the incident involving personnel records announced on June 4th. All notices have been sent by letter or email. Notification letters were sent by first class mail late last week to those individuals from whom an email bounce back message was received.

As we have mentioned in our previous communications, OPM is offering credit monitoring services and identity theft insurance with CSID, a company that specializes in identity theft protection and fraud resolution. This comprehensive, 18-month membership includes credit report access, credit monitoring, identity theft insurance, and recovery services, and is available immediately at no cost to affected individuals identified by OPM.

All affected employees are *automatically* enrolled in identity theft insurance with \$1 million in potential coverage and identity restoration services – which means that if your information was affected by the breach, *you are already enrolled in these programs even if you have not yet contacted CSID.*

Affected employees are also being provided *the option to sign up* through CSID for credit monitoring and other identity monitoring services. To take advantage of these additional free services, employees will have call and register with CSID. The FAQs below provide some more detail on these services.

We encourage State employees who want to sign up for credit monitoring and other identity monitoring services to wait until they receive notifications before calling CSID to allow for

others who were notified and need technical assistance to get through. Notifications may still take several days to arrive as we are still sending letters to a number of individuals. Once OPM has completed these mailings, we will provide you with information on how to contact CSID if you think you should have been notified, but have not been.

As mentioned, we have heard your concerns regarding these notifications and CSID's customer service – and we have been working with OPM to improve the quality of your experience. We understand that many of you are concerned about providing PII to CSID to register for this service. OPM has confirmed that it is not possible for CSID to provide credit monitoring services without your Social Security Number, but that you will still receive identity theft protection even if you do not register.

OPM is continuing to work with CSID to make the online signup experience quicker and to reduce call center wait times. These efforts include expanding staffing and call center hours, and increasing server capacity to better handle on-line sign ups at peak times. CSID has indicated that wait times are dependent on the volume of calls, which are usually highest between 9 a.m. and 10 a.m. CST and from noon to 1 p.m. CST.

Background Investigation Incident

Second, regarding the separate but related cyber incident affecting background investigations announced on June 12th, we understand that many of you are concerned and seeking more information. This incident remains under investigation by OPM, the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI). The investigators are working to determine the complete list of affected individuals. Once this information is available, OPM will coordinate with agencies to send notifications to those affected individuals as soon as possible, but this will take some time. We expect to be ready to provide information regarding affected individuals and our notification process during the week of July 6th.

EQIP SUSPENSION

OPM today announced the temporary suspension of the E-QIP system, a web-based platform used to complete and submit background investigation forms. The suspension is to enable OPM to implement security enhancements.

The actions OPM has taken are not the direct result of malicious activity on this network, and there is no evidence that the vulnerability in question has been exploited. Rather, OPM is taking this step proactively, as a result of its comprehensive security assessment, to ensure the ongoing security of its network.

OPM expects e-QIP could be offline for four to six weeks while these security enhancements are implemented. OPM recognizes and regrets the impact on both users and agencies and is committed to resuming this service as soon as it is safe to do so. In the interim, OPM remains committed to working with its interagency partners on alternative approaches to address agencies' requirements.

Resources for You

OPM also continues to update their Frequently Asked Questions which you can find here: www.opm.gov/cybersecurity

We encourage you to review OPM Director Katherine Archuleta's recent blog which also addresses many of these concerns: <http://www.opm.gov/blogs/Director>. OPM is the definitive source for information on the recent cyber incidents and we will continue to update you as we learn more information. We remain interested in your feedback and questions on the incident and our communications. You can reach out to us at DG Direct [DGDIRECT@STATE.GOV] with these comments.

Personal Safety and Cybersecurity Reminders

The following are also some key reminders of the seriousness of cyber threats and of the importance of vigilance in protecting our systems and data.

Safety of Personal Information Resources from National Counterintelligence and Security Center:

- Employees can find information about the measures they can take to ensure the safety of their personal information at the National Counterintelligence and Security Center (NCSC) at <http://www.ncsc.gov>.

Steps for Monitoring Your Identity and Financial Information

- Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. Consumers are entitled by law to one free credit report per year from each of the three major credit bureaus – Equifax®, Experian®, and TransUnion® – for a total of three reports every year. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) website, www.ftc.gov.
- Review resources provided on the FTC identity theft website, www.Identitytheft.gov. The FTC maintains a variety of consumer publications providing comprehensive information on computer intrusions and identity theft.
- You may place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call TransUnion® at 1-800-680-7289 to place this alert. TransUnion® will then notify the other two credit bureaus on your behalf.

Precautions to Help You Avoid Becoming a Victim

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, <http://www.us-cert.gov/ncas/tips/ST04-013>).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (<http://www.antiphishing.org>).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, <http://www.us-cert.gov/ncas/tips/ST04-004>; Understanding Anti-Virus Software, <http://www.us-cert.gov/ncas/tips/ST04-005>; and Reducing Spam, <http://www.us-cert.gov/ncas/tips/ST04-007>).
- Take advantage of any anti-phishing features offered by your email client and web browser.
- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.
- Additional information about preventative steps by consulting the Federal Trade Commission's website, www.consumer.gov/idtheft. The FTC also encourages those who discover that their information has been misused to file a complaint with the commission using the contact information below.

Identity Theft Clearinghouse
 Federal Trade Commission
 600 Pennsylvania Avenue, NW
 Washington, DC 20580
<https://www.identitytheft.gov/>
 1-877-IDTHEFT (438-4338)
 TDD: 1-202-326-2502